SNMP Authentication

SNMP Policies

Cisco UCS Central supports:

- Global SNMP policies
- Defining SNMP traps and informs
- Defining SNMP users

You can define them with regular and privacy passwords, authentication types of MD5 or SHA, and encryption types DES and AES-128. Registered Cisco UCS domains choosing to define SNMP policies globally within that client's policy resolution control defer all SNMP policies to its registration with Cisco UCS Central.

The SNMP Agent functionality remotely monitors Cisco UCS Central. You can also change the Cisco UCS Central host IP, and then restart the SNMP agent on the new IP. SNMP is run on both the active and standby Cisco UCS Central servers. The configuration persists on both. Cisco UCS Central offers read-only access to only the operating system managed information base (MIB). Through the Cisco UCS Central CLI you can configure the community strings for SNMP v1, v2c, and create and delete the SNMPv3 users.

SNMP Functional Overview

The SNMP framework consists of three parts:

SNMP Manager

System used to control and monitor the activities of network devices using SNMP.

SNMP Agent

Software component within Cisco UCS Central. The managed device that maintains the data for Cisco UCS Central and reports the data, as needed, to the SNMP manager. Cisco UCS Central includes the agent and a collection of MIBs. To enable the SNMP agent and create the relationship between the manager and agent, enable and configure SNMP.

Managed Information Base (MIB)

Collection of managed objects in the SNMP agent. Cisco UCS Central supports only the OS MIBs.

For information about the specific MIBs available for Cisco UCS and where you can obtain them, see the MIB Reference for Cisco UCS Manager for B-series servers, and MIB Reference for Cisco UCS Standalone C-Series Servers C-series servers.

The following RFCs define the SNMP:

- RFC 3410 (http://tools.ietf.org/html/rfc3410)
- RFC 3411 (http://tools.ietf.org/html/rfc3411)
- RFC 3412 (http://tools.ietf.org/html/rfc3412)
- RFC 3413 (http://tools.ietf.org/html/rfc3413)
- RFC 3414 (http://tools.ietf.org/html/rfc3414)
- RFC 3415 (http://tools.ietf.org/html/rfc3415)
- RFC 3416 (http://tools.ietf.org/html/rfc3416)
- RFC 3417 (http://tools.ietf.org/html/rfc3417)
- RFC 3418 (http://tools.ietf.org/html/rfc3418)
- RFC 3584 (http://tools.ietf.org/html/rfc3584)

SNMP Notifications

A key feature of SNMP is the ability to generate notifications from an SNMP agent. These notifications do not require that the SNMP manager send the requests. Notifications can indicate improper user authentication, restarts, the closing of a connection, loss of connection to a neighbor router, or other significant events.

Cisco UCS Central generates SNMP notifications as traps. Traps are less reliable than Informs because the SNMP manager does not send any acknowledgment when it receives a trap. Therefore, Cisco UCS Central cannot determine if it received the trap.

An SNMP manager that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If Cisco UCS Central does not receive the PDU, it can send the inform request again.

SNMP Security Features

SNMPv3 provides secure access to devices through a combination of authenticating and encrypting frames over the network. SNMPv3 authorizes management operations only by configured users and encrypts SNMP

messages. The SNMPv3 user-based security model (USM) refers to SNMP message-level security and offers the following services:

Message Integrity

Ensures that nothing has altered or destroyed any messages in an unauthorized manner. Also ensures that nothing has altered data sequences to an extent greater than can occur non-maliciously.

Message Origin Authentication

Confirms the claimed identity of the user who received the data.

Message Confidentiality and Encryption

Ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.

SNMP Security Levels and Privileges

SNMPv1, SNMPv2c, and SNMPv3 each represent a different security model. A security model is an authentication strategy that is set up for a user and the role in which the user resides. The security model combines with the selected security level to determine the security mechanism applied when Cisco UCS Central processes the SNMP message.

The security level determines the privileges required to view the message associated with an SNMP trap. The security level determines whether Cisco UCS Central must protect the message from disclosure, or authenticate it. The supported security level depends upon which security model is implemented. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet. SNMP security levels support one or more of the following privileges:

NoAuthNoPriv

No authentication or encryption.

AuthNoPriv

Authentication but no encryption.

AuthPriv

Authentication and encryption.

SNMPv3 provides for both security models and security levels.

SNMP Security Models and Levels

The following table describes the combinations of SNMP security models and levels supported in Cisco UCS Central.

Table 1: SNMP Security Models and Levels

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	HMAC-MD5 or HMAC-SHA	No	Provides authentication based on: • Hash-based Message Authentication code (HMAC) • Message Digest 5 (MD5) algorithm • HMAC Secure Hash algorithm (SHA)

Model	Level	Authentication	Encryption	What Happens
v3	authPriv	HMAC-MD5 or HMAC-SHA	DES	Provides authentication based on: • Hash-based Message Authentication code (HMAC) • Message Digest 5 (MD5) algorithm • HMAC Secure Hash algorithm (SHA) • Provides Data Encryption Standard (DES) 56-bit encryption. • Provides authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.

SNMP Support in Cisco UCS Central

Support for MIBs

Cisco UCS Central supports read-only access to OS MIBs. No set operations are available for the MIBs. The following MIBs are supported by Cisco UCS Central:

- SNMP MIB-2 System
- HOST-RESOURCES-MIB
  - hrSystem
  - hrStorage

    - hrDevice
    - hrSWRun
    - hrSWRunPerf
- UCD-SNMP-MIB
    - Memory
    - dskTable
    - systemStats
    - fileTable
- SNMP MIB-2 Interfaces
    - ifTable
- IP-MIB
- SNMP-FRAMEWORK-MIB
    - snmpEngine
- IF-MIB
- DISMAN-EVENT-MIB
- SNMP MIB-2 snmp

Note Cisco UCS Central does not provide support for IPV6 and Cisco UCS Central MIBs.

Authentication Protocols for SNMPv3 Users

Cisco UCS Central supports the following authentication protocols for SNMPv3 users:

- HMAC-MD5-96 (MD5)
- HMAC-SHA-96 (SHA)

AES Privacy Protocol for SNMPv3 Users

Cisco UCS uses Advanced Encryption Standard (AES) as one of the privacy protocols for SNMPv3 message encryption and conforms with RFC 3826.

The privacy password, or priv option, offers a choice of DES or 128-bit AES encryption for SNMP security encryption. If you enable AES-128 configuration and include a privacy password for an SNMPv3 user, Cisco UCS Central uses the privacy password to generate a 128-bit AES key. The AES privacy password can have a minimum of eight characters. If the passphrases are specified in clear text, you can specify a maximum of 64 characters.

Enabling SNMP

Procedure

Step 1 Click the **System Configuration** icon and choose **SNMP**.
This launches the **UCS Central SNMP Manage** dialog box.

Step 2 On the **Basic** tab, select **Enabled** or **Disabled**. If you selected **Enabled**, complete the following fields.

a) In **Community/User Name**, enter the default SNMP v1 or v2c community name or SNMP v3 username.

b) In **System Contact**, enter the system contact person responsible for the SNMP implementation.
Enter a string of up to 255 characters, such as an email address or a name and telephone number.

c) In **System Location**, enter the location of the host on which the SNMP agent (server) runs.
Enter an alphanumeric string up to 510 characters.

Step 3 Click **Save**.

What to Do Next

Create SNMP traps and users.

Creating and Editing an SNMP Trap or Inform

After creating an SNMP trap, you can edit the SNMP trap information as required.

Procedure

Step 1 Click the **System Configuration** icon and choose **SNMP**.
This launches the **UCS Central SNMP Manage** dialog box.

Step 2 On the **SNMP Traps** tab, click **Add**.

Step 3 In **Trap Host Name/IP Address**, enter the IP address of the SNMP host to which to send the trap.

Step 4 In **SNMP Trap Properties**:

a) In **Community/User Name**, enter the default SNMP v1 or v2c community name or SNMP v3 username.

b) In **Port**, enter the port on which the system communicates with the SNMP host for the trap.
Enter an integer between 1 and 65535. The default port is 162.

c) For **Version**, select **V1**, **V2C**, or **V3**.

d) If you selected V2C or V3, then for **Type**, select **Traps** or **Informs**.

e) If you selected V3, then select the **V3Privilege**:

- **Auth—**Authentication but no encryption
- **NoAuth—**No authentication or encryption
- **Priv—**Authentication and encryption

Step 5 Click **Save**.

What to Do Next

Create an SNMP user.

Creating and Editing an SNMP User

After creating an SNMP user, you can edit the SNMP user information as required.

Procedure

Step 1 Click the **System Configuration** icon and choose **SNMP**.
This launches the **UCS Central SNMP Manage** dialog box.

Step 2 On the **SNMP Users** tab, click **Add**.

Step 3 In **SNMP User Name**, enter the username assigned to the SNMP user.
Enter up to 32 letters or numbers. The name must begin with a letter and you can also specify _ (underscore), . (period), @ (at sign), and - (hyphen).

Step 4 In **SNMP User Properties**:

a) In **Authentication Type**, select the **MD5** or **SHA** as the authorization type.
b) For **AES-128 Encryption**, click **Enabled** or **Disabled**.
c) Enter and confirm the **Password** and **Privacy Password**.

Step 5 Click **Save**.